網路程式設計-期中考(2020.11.20)-破密碼

1. 請加入引入檔於程式中，

例(Ex): **#include “TCPIP\_Sync.cpp”**

**#include “MD5.c”**

1. 使用TCP(Port=6000)連線伺服器140.113.144.227。

例(Ex): Start\_TCP\_Client(…)

1. 請使用下列格式送出註冊指令(REGISTER/姓名/學號)。

範例: strcpy\_s(S1,“REGISTER/王大明/1090123”);

send(Sock,S1,strlen(S1),0);

1. 您將收到 “註冊成功/16-Bytes Hash”之訊息

範例: “註冊成功/3df5e3812619a480202795efbedc693a”

此16-Bytes Hash是由介於[0~32767]整數經過200次MD5攪亂(Hash)之結果

以 “16146”為例，遞迴將輸出再帶進輸入跑200次:

1st: MD5\_Encoder(“16146”,Resp); //Resp=“b996f9609f0750e3bbdf52445a22cfc1”

2nd: MD5\_Encoder(“b996f9609f0750e3bbdf52445a22cfc1”,Resp); //Resp=“890a752b53cdbbddd7828c143b2ecd41”

3rd: MD5\_Encoder(“890a752b53cdbbddd7828c143b2ecd41”,Resp); //Resp=“2dcbb3071e04a985896022f96f05cc41”

4th: MD5\_Encoder(“2dcbb3071e04a985896022f96f05cc41”,Resp); //Resp=“b781c41ec0f4c54b1717d912983d2f0d”

…

200th: MD5\_Encoder(“99e10ad82c7ac65a5b7e0605bd3b01e7”,Resp); //Resp=“3df5e3812619a480202795efbedc693a”

註1: 也就是說 “16146” 做MD5 演算法200次，可以得到 “3df5e3812619a480202795efbedc693a”，

MD5200(“16146”)= “3df5e3812619a480202795efbedc693a”

註2: 而MD5是一個不可逆的雜湊函式，若獲得Resp=“3df5e3812619a480202795efbedc693a”，想要逆向推出“16146”是不

可能的，只能用暴力破解法將0~32767間之值一個個帶入遞迴算200次，看誰的產出符合Resp

1. 您在第4步收到的16-Bytes Hash是由一個介於[0~32767]之數字(Key)經過200次MD5\_Encoder所產生的Hash，因此您必須在第4步收到16-Bytes Hash後，利用暴力攻擊法找出介於[0~32767]之Key。(註:暴力攻擊需要十餘秒時間計算出Key)
2. 使用下列指令格式將找出的Key傳給伺服器

例: “ANSWER/姓名/學號/Key”

範例: sprintf\_s(S1,“ANSWER/王大明/1090123/%d”,Key);

send(Sock,S1,strlen(S1),0);

1. 請接收伺服器回傳之作答結果